Cybersécurité – Réglementation

Sensibilisation aux réglementations, normes et bonnes pratiques liées à la Cybersécurité

Cette formation de 2 jours « **Sensibilisation aux réglementations liée à la cybersécurité** » est destinée aux **dirigeants d'ETI, PME, TPE, Startups et collectivités** ayant des connaissances élémentaires en informatique et information générale en cybersécurité.

Le programme propose une immersion approfondie dans le monde complexe de la cybersécurité, combinant la **sensibilisation aux réglementations avec une exploration pratique des menaces et des meilleures pratiques de sécurité**.

L'objectif est de fournir aux participants une **connaissance approfondie des normes de cybersécurité** tout en favorisant une **compréhension pratique des risques et des solutions concrètes**, essentielles pour les professionnels.

Objectifs

Fournir une vue d'ensemble complète de la réglementation	Comprendre les principes et la mise en œuvre ISO 27001 et directives NIS2 et DORA	Mettre en pratique le NIST Framework et répondre aux défis de la RGPD	Explorer les réglementations complémentaires et conformités intersectorielles	Renforcer ses compétences par une application pratique

Publics cibles

Ce parcours est ouvert aux dirigeants d'ETI, PME, TPE, Startups et collectivités ayant des connaissances élémentaires en informatique et un niveau d'information général en cybersécurité.

Pré-requis et objectifs pédagogiques

Aucune connaissance préalable spécifique en cybersécurité est nécessaire pour aborder les objectifs pédagogiques suivants :

- Explorer les normes majeures de cybersécurité
- Appliquer les principes de l'ISO 27001 et des directive NIS2 et DORA dans des contextes réels
- Mettre en pratique le NIST Framework pour renforcer la sécurité des données
- Examiner et comprendre les réglementations complémentaires telles que IA Act, HIPAA et PCI-DSS
- Développer les compétences pratiques par le biais d'ateliers

Programme

Cette formation se démarque par son approche pratique et opérationnelle.

Elle est proposée en présentiel, dure 14 heures, et est déployée sur deux journées consécutives.

Axée sur les réglementations liées à la cybersécurité elle combine une vue d'ensemble, une sensibilisation aux normes et à la RGPD, appuyée par des études de cas concrets pour permettre une meilleure compréhension et application des connaissances.

1. Exploration des normes et concrétisation des pratiques

> Introduction Interactive à la cybersécurité

> Normes de Cybersécurité en Action

Introduction approfondie aux normes majeures : ISO 27001, NIST, RGPD, NIS2, DORA

Analyse des mécanismes de conformité, en mettant l'accent sur la réduction des risques

Exemples concrets tirés de cas réels, illustrant la conformité et les conséquences en cas de non-conformité.

2. Exploration pratique de la norme ISO 27001 et des directives NIS2 et DORA

Atelier interactif sur la mise en œuvre de l'ISO 27001 et des directives NIS2 et DORA

Approfondissement des principes de gestion des risques et de classification des informations pour minimiser les vulnérabilités.

Retours d'expérience concrets et partage des meilleures pratiques pour optimiser les processus et systèmes.

3. Mise en Lumière du NIST Framework et de la RGPD :

Session interactive sur l'application concrète du NIST Framework avec une perspective sur les projets de conformité

Discussions sur les implications de la RGPD, mettant en avant les opportunités de dérisquage des pratiques.

Scénarios interactifs détaillant la conformité avec la RGPD, en soulignant les bonnes pratiques de protection des données.

4. Réglementations complémentaires (IA Act, HIPAA, PCI-DSS)

Vue d'ensemble interactive d'autres réglementations telles que lA Act, HIPAA et PCI-DSS

Discussions approfondies en groupe sur les exigences spécifiques de ces réglementations.

5. Découverte des menaces et renforcement des pratiques sécuritaires :

> Sensibilisation aux Menaces Courantes et Risques

Exploration interactive des menaces courantes avec une focalisation sur la sensibilisation des équipes.

Analyse approfondie et identification des risques spécifiques aux TPE, intégrant des pratiques dérisquantes, pour renforcer la posture de sécurité de l'organisation, et mettre l'accent sur la projection vers un futur sécurisé.

Conséquences financières et opérationnelles des attaques.

6. Techniques d'attaque et pratiques préventives :

Exploration interactive des techniques d'attaque, incluant le phishing, les ransomwares, etc.

Études de cas approfondies avec identification de signaux précurseurs, mettant l'accent sur la détection précoce.

Conseils détaillés sur les bonnes pratiques de sécurité, avec une orientation dérisquante.

7. Protection et réaction aux cybermenaces :

Développement interactif d'un plan d'action en cas d'incident cybernétique.

Méthodologie interactive pour identifier, isoler et résoudre rapidement les incidents, minimisant les pertes.

Sensibilisation interactive à la communication et à la notification des incidents, intégrant des stratégies de dérisquage.

8. Solutions de Protection Accessibles aux ETI, PME, TPE, Stratups :

Présentation interactive des outils et logiciels abordables pour renforcer la sécurité.

Sélection interactive de solutions en fonction des besoins et des budgets des ETI, PME, TPE et startups.

Démo interactive d'antivirus efficaces basée sur des cas d'utilisation réels.

9. Développement d'une culture de sécurité au sein des petites entreprises :

Sensibiliser et former votre personnel aux bonnes pratiques de sécurité.

Mise en place de processus internes favorisant une culture de sécurité continue, orientée vers un avenir résilient face aux défis cybernétiques.

Illustration interactive de la mise en place de processus internes pour signaler les incidents de sécurité et y réagir rapidement.

Compétences ciblées

- Comprendre et appliquer les normes majeures de cybersécurité pour assurer la conformité et réduire les risques
- Evaluer les risques spécifiques à son organisation, définir des stratégies de gestion des risques efficaces et mettre en œuvre des mesures de mitigation adaptées
- Comprendre et respecter les réglementations complémentaires telles que HIPAA et PCI-DSS, et les intégrer dans sa politique de cybersécurité
- Sensibiliser et former les collaborateurs aux bonnes pratiques de sécurité, instaurer une culture de sécurité continue et réagir efficacement en cas d'incident
- Sélectionner et déployer des outils de protection adaptés

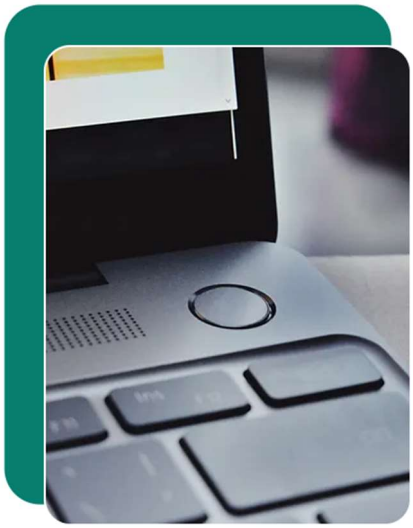
Moyens pédagogiques

Cette **formation sur mesure destinée aux ETI, PME, TPE, Startups et collectivités** se démarque par son approche pratique et opérationnelle.

Axée sur une sensibilisation aux réglementations elle combine des présentations interactives et des études de cas concrets pour **offrir une vision précise des normes**.

Les **démonstrations pratiques** mettent l'accent sur **l'application directe des normes**, tandis que les sessions interactives encouragent une participation active. Ces séquences incluent également une **mise en application des connaissances** dans des situations réelles.

En outre, des **supports visuels clairs et pertinents** viennent enrichir cette expérience d'apprentissage, **offrant des solutions tangibles** pour **protéger efficacement une entreprise**.



Moyens d'encadrement

La formation est assurée par un formateur.rice expert.e en cybersécurité, disposant d'une expérience professionnelle significative sur la thématique et une expérience en techniques d'animation.

Modalités d’évaluation

Les évaluations se dérouleront à travers des tests pratiques simplifiés évaluant la compréhension des principes de sécurité fondamentaux.

Le dispositif d’évaluation est composé de :

- Questionnaires à choix multiples pour évaluer les connaissances théoriques sur les normes et leur utilisation.
- Des mini exercices pratiques afin de déterminer ce qu’il est pertinent de mettre en place en fonction de son organisation.

Ces méthodes d'évaluation permettront de mesurer la compréhension, la réactivité et l'application des connaissances acquises lors de la formation.

Une **attestation de réalisation** est remise à chaque participant **à l’issue de la formation**. Une attestation de réussite est remise aux participants satisfaisant les critères de réussite de la formation.

Prix et modalités d'accès

La formation est commercialisée en inter-entreprise et en intra-entreprise pour des groupes de 6 à 12 personnes.

Prix HT : à partir de 1550 €

Innov8learn
98 rue du Château - 92100 Boulogne-Billancourt